The HIPAA Implementation Newsletter
Issue #43 – Friday, October 5, 2002
| Privacy | Security | Business Associates | HIPAA & Physicians
Web format with links at http://lpf.com/hipaa

Privacy: Culture

Effective privacy and security requires the establishment or enhancement of a culture of concern for the protection of information. A culture has self sustaining characteristics and successes breed a stronger culture. The alternative is a set of rules that have to be imposed on people and periodically reinforced. For that reason, we are recommending to our clients that the privacy policies and procedures required by HIPAA have only a minimum linkage to the rules of HIPAA. (See following article.)

If clients do not already have a clearly appropriate place to put the new policies and procedures, we are recommending a new Privacy & Security Policies and Procedures Manual. In the introduction, the manual states that the purpose is to foster and encourage a culture of concern for the protection of patient, staff and organizational information. It notes that the policies and procedures in this manual are in compliance with HIPAA where applicable.

Privacy: Tools

The regulations for privacy will change and regulations for security will be added. We are recommending that clients create and maintain a *Regulation Traceability Matrix.* The matrix should have five columns: policy, regulation, regulation date, state law, and state law date. The *policy* column should show the name and reference, e.g., page number or policy number, to a specific policy. The *regulation* column should list the section or sections of the regulation that apply to a particular policy. The *regulation date* should be the date of the regulation; as an example, either of the two final privacy regulations. The *state law* column should note that the policy is based on a state law that preempts the regulation, is based on the regulation and counsel has determined that state law is preempted, or that state law is not applicable with regard to this regulation. The *state law date* is the date of the state law. The data should be maintained in an Excel spreadsheet or other format that can be sorted to facilitate identification of items that may need to be revised. As an example, if a HIPAA regulation is revised the list could be sorted by regulation, policies affected by the revision regulation could be identified and updated and the matrix could be updated to reflect those changes.

Privacy: Sports

"Claude Allen, deputy secretary of Health and Human Services, said Tuesday, 'I doubt seriously that information the way it's currently issued will change substantially.' If there are privacy problems for teams regarding the Health Insurance Portability and Accountability Act, Allen said the issues could be solved by applying for a waiver or inserting provisions into contracts or scholarships. Allen said most of the major sports bodies in the USA have requested a meeting with HHS, probably next month.

THE LAW OF UNINTENDED CONSEQUENCES: "Because of the clampdown, concern for gamblers trying to find out information is heightened. 'This year in particular, I personally spoke with the team and the staff and reminded them that changes are

on the horizon and this is a concern, and we would be foolish and naive to think gambling doesn't exist and there may be times when you'll be approached by somebody who wants to know about an athlete's playing condition,' Clements said. 'Tell them to say they don't know anything; it's none of their business.'"
+ More at: http://www.usatoday.com/usatonline/20020925/4478780s.htm

Security: Network Worms

"W32/Bugbear, which travels via e-mail and network shares, is also called Tanat, Tanatos, and WORM_NATOSTA.A. Antivirus vendor F-Secure is seeing as many reports of Bugbear as Klez, the most prevalent worm of the last six months, said Mikko Hypponen, F-Secure's manager of antivirus research.

"There are two dangers associated with Bugbear. First, the worm opens a backdoor and installs a keystroke-logging program on infected systems, giving it the ability to harvest passwords and other sensitive information. Additionally, Bugbear aggressively targets antivirus and firewall software. The worm periodically tries to shut down processes associated with popular antivirus and firewall products. …

"Bugbear spreads by sending itself as an e-mail attachment and through network file shares. The latter functionality may have something to do with its success, because only one user on a network has to open the attachment. Once a machine is infected, the worm can spread itself throughout the network. This is not just an issue for corporations. Home DSL and cable users [read trusted small providers and business associates] could become infected [and cause infections] via this method ….

"The worm also steals e-mail messages from infected systems and forwards them with copies of itself. The use of real e-mails lends some credibility to the messages, which prompts some recipients to open it. The technique could also send out sensitive information, Hypponen said.

"Another new worm that uses network shares to spread and can install a backdoor in systems was discovered on Tuesday: … It's also called Opasoft. Windows 9x systems are affected but Windows NT systems are not. W32.Opaserv.Worm is a network-aware worm that attempts to replicate across open network shares. It copies itself to the remote computer as a file named Scrsvr.exe."

The HIPAA Act requires "Each person … shall maintain reasonable and appropriate administrative, technical, and physical safeguards … to ensure the integrity and confidentiality of the information [and] … to protect against any reasonably anticipated threats or hazards to the security or integrity of the information …" These types of worms are now common enough that they fall within the realm of "reasonably anticipated threats." We are recommending that our clients consider including appropriate safeguards in business associate contracts where information is currently or may be transmitted via a network connection.

Business Associates: Chain of Trust

"Now is not the time to ask business associates to sign chain of trust agreements. The security rule is not yet final, so you won't know exactly what to include. Instead, put language in your business associate contracts that allows you to add chain of trust agreements once the security rule is finalized, says Gretchen McBeath, JD, partner in the health care department at Bricker and Eckler, LLP, in Columbus, OH.

"Chain of trust agreements are the security equivalent of business associate agreements and can be fairly technical because they outline the specific security measures that entities sharing and exchanging PHI will use to protect the integrity of information. Chain of trust agreements pertain only to information transferred electronically.
"Hospitals and health plans will have to establish business associate agreements with their auditors, lawyers, and coding consultants, she says."[But] typically, those services won't always involve the electronic exchange of information." If they don't, you won't need a chain of trust agreement.
"McBeath recommends you do the following:
1. Take your business associate inventory a step further. Once you've put together a list of your facility's business associates, determine which ones send and receive patient information electronically. They will eventually need chain of trust agreements. …
2. Preserve the option to add an agreement. In your business associate agreements with every company on the list, add a provision that allows you to modify the contract and add chain of trust language. … The best thing to do is to include language in a business associate agreement that says both parties agree that the [contract] will be amended to comply with any future rules.
3. Look for further guidance. … I suspect that HHS will issue a model agreement, because they issued a model business associate agreement language and a model notice of privacy practices.
"This week's HIM Connection was adapted from the newly updated special report, "Managing Your Business Associates: Ensure that your partners are HIPAA-compliant." Go to http://www.hcmarketplace.com/Prod.cfm?id=1065&s=EHIMC for more information on this resource for HIM professionals."
+ Subscription to HIM Connection:
http://www.hcmarketplace.com/free/emailnls.cfm

HIPAA and Physicians

"Headaches ahead. that's what the chief administrative officer for a 10-doctor practice in the San Francisco Bay area, predicts for the Health Insurance Portability and Accountability Act when it rolls out across the United States next year. But more for patients than providers. 'People are used to calling in to get insurance, billing or health information for themselves, their children, spouses or bosses. … They won't be able to do that anymore. To me, the biggest challenge will be reeducating people about what the law will mean for them. They need to understand that as providers, we may not be able to do some things as quickly as we have in the past.'

"Developing educational materials to help patients get their arms around the changes HIPAA will bring is just one of the items on physicians' to-do list these days. As operational, procedural and technical preparations for compliance continue, providers' challenges abound.

"Separating Truth From Rumors

- What about calling patient names in the waiting room? Patients' names can be called out in the waiting room as long as a diagnosis, treatment or reason for being in the offices is not associated with a name.

- Is it OK to have a visit log that patients sign in on when they enter the office? Yes, a log is authorized, but it cannot have diagnosis, treatment, or symptoms information corresponding to the patient's name or demographics.

• Do we need to build a separate room to secure the patient charts? No, you do not need to have a highly secure room, but you need to have processes defined and in place that protect private health information from exposure to those not authorized to see it."
+ More at:
http://www.healthleaders.com/magazine/feature1.php?contentid=37831&CE_Session=ea506f4aa48175274cb27a042bd4b976
National HIPAA Audio conference: Donna Eden, Esq., DHHS Office Of General Counsel, addresses employer HIPAA extension plan filing & compliance strategies Oct. 8, 2002 10:00 am - 11:30 am PDT (and Arizona)… 1:00 pm - 2:30 pm EDT -- Sponsored by: Health Affairs, http://www.HealthAffairs.org, Alliance of Community Health Plans, http://www.achp.org, Blue Cross/Blue Shield Association, http://www.bcbs.com, Consumer Driven Healthcare Association, http://www.cdhca.org, National Business Coalition on Health, http://www.nbch.org, National Committee on Quality Assurance, http://www.ncqa.org, & Pacific Business Group on Health, http://www.PBGH.org -- 11 Categories Of Continuing Education Credit Offered: http://www.HIPAAAudioconferences.com

The fifth National HIPAA Summit, October 30 - November 1, 2002 in Baltimore, MD, http://www.HIPAASummit.com At a special session on Thursday morning, Oct. 31, 2002, federal and state regulators of healthcare privacy and security experts will provide regulatory updates, and respond to questions and comments. From the Dept Of Health & Human Services, the White House, the Federal Trade Commission, the National Association Of Insurance Commissioners, and from North Carolina, New York, the Southern HIPAA Administrative Regional Process (SHARP), NCHICA, Indiana HIPAA Consortium, National Association of Health Data Organizations, Massachusetts Health Data Consortium, Inc, and a group of national experts.
